INTERNATIONAL SEARCH REPORT

PCT/IB2004/050888

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2001/034837 A1 (KAUSIK BALAS NATARAJAN ET AL) 25 October 2001 (2001-10-25) abstract paragraph '0007! paragraph '0023! paragraph '0032! claim 16	1-14
X	MENEZES,VANSTONE,OORSCHOT: "Handbook of Applied Cryptography" 1997, CRC PRESS LLC , USA , XP002296714 page 397 page 400 - page 417	1-14

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 September 2004	08/11/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	San Millán Maeso, J

INTERNATIONAL SEARCH REPORT

PCT/IB2004/050888

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2001034837 A1	25-10-2001	US 6263446 B1	17-07-2001
		US 6170058 B1	02-01-2001
		AU 1631200 A	05-06-2000
		BR 9915474 A	31-07-2001
		CA 2347893 A1	25-05-2000
		CN 1354929 T	19-06-2002
		EP 1131911 A1	12-09-2001
		JP 2002530930 T	17-09-2002
		NO 20012463 A	18-05-2001
		NZ 511397 A	28-03-2003
		WO 0030285 A1	25-05-2000
		AU 746966 B2	09-05-2002
		AU 2097399 A	12-07-1999
		CA 2314349 A1	01-07-1999
		EP 1048143 A1	02-11-2000
		JP 2001527325 T	25-12-2001
		NO 20003310 A	22-08-2000
		WO 9933222 A1	01-07-1999
		US 2001008012 A1	12-07-2001